Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A semiconductor integrated circuit, provided as a monolithic circuit, for decryption of broadcast signals, comprising:

an input interface for receipt of received encrypted broadcast signals, a broadcast encrypted common key, and broadcast control data, and an output interface for output of decrypted broadcast signals;

a processing unit arranged to receive encrypted broadcast signals via the input interface, to decrypt the encrypted broadcast signals in accordance with control signals, and to provide decrypted broadcast signals to the output interface;

a first decryption circuit arranged to receive encrypted control signals from the input interface and to decrypt the control signals in accordance with a decrypted common key from a dedicated common key store in the integrated circuit; and

a second decryption circuit arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key from a secret key store in the integrated circuit;

whereby the circuit is arranged such that the only route to placing a common key in the common key store is to ~~input~~ receive by broadcast the common key in encrypted form for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

2. (Original) The semiconductor integrated circuit of claim 1, wherein the first decryption circuit and second decryption circuit are formed in a common circuit.

3. (Original) The semiconductor integrated circuit of to claim 1, wherein at least one of the first decryption circuit and the second decryption circuit comprises an AES circuit.

4. (Original) The semiconductor integrated circuit of claim 1, wherein the broadcast signal comprises a digital television signal and the processing unit comprises a DVB circuit.

5. (Original) The semiconductor integrated circuit of claim 1, wherein the input interface has a separate input for the encrypted common key connected to the decryption circuit.

6. (Original) The semiconductor integrated circuit of claim 1, wherein the secret key is unique to the semiconductor integrated circuit.

7. (Original) The semiconductor integrated circuit of claim 1, wherein the common key store is arranged to store multiple common keys.

8. (Original) A television decoder comprising the semiconductor integrated circuit of claim 1.

9. (Currently Amended) A system for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals, the system comprising:

a transmitter arranged to broadcast:

signals encrypted according to control words;

control words encrypted according to a common key common to two or more authorized recipients; and

a common key encrypted respectively according to a unique secret key of each authorized recipient;

the system further comprising a plurality of receivers, each comprising a semiconductor integrated circuit ~~according to claim 1~~, wherein the secret key is unique to each semiconductor integrated circuit, the semiconductor integrated circuit comprising:

an input interface for receipt of received encrypted broadcast signals, a broadcast encrypted common key, and broadcast control data, and an output interface for output of decrypted broadcast signals;

a processing unit arranged to receive encrypted broadcast signals via the input interface, to decrypt the encrypted broadcast signals in accordance with control signals, and to provide decrypted broadcast signals to the output interface;

a first decryption circuit arranged to receive encrypted control signals from the input interface and to decrypt the control signals in accordance with a decrypted common key from a dedicated common key store in the integrated circuit; and

a second decryption circuit arranged to receive the common key in encrypted form from the input interface and to decrypt the common key in accordance with a secret key from a secret key store in the integrated circuit;

whereby the circuit is arranged such that the only route to placing a common key in the common key store is to receive by broadcast the common key in encrypted form for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

10. (Currently Amended) A ~~monolithic~~ set top decoder device for decryption of broadcast signals, comprising:

a monolithic device located in the set top box;

a common key store in the monolithic device and configured to receive a broadcast common key;

a secret key store in the monolithic device configured to store a secret key;

a decryption unit comprising a first decryption circuit configured to receive encrypted broadcast control signals and to decrypt the control signals in accordance with the common key from the common key store, and a second decryption circuit configured to receive the broadcast common key in encrypted form and to decrypt the common key in accordance with a secret key from the secret key store and to store the decrypted common key in the common key store; and

a processing unit configured to receive encrypted broadcast signals and decrypt the encrypted broadcast signals in accordance with the decrypted control signals received from the decryption unit and to provide decrypted broadcast signals to an output interface;

whereby the device is arranged such that the only route to placing a common key in the common key store is to input the common key in encrypted form for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

11. (Original) The device of claim 10, wherein the common key store is configured to store multiple common keys.

12. (Original) The device of claim 10, wherein the decryption device is formed as a single semiconductor integrated circuit having an input interface for receipt of encrypted broadcast signals, encrypted control signals, and encrypted common keys, and an output interface for output of decrypted broadcast signals.

13. (Currently Amended) A method of decrypting encrypted broadcast signals, comprising:

receiving encrypted broadcast signals, encrypted broadcast control signals, and encrypted broadcast common key signals at an input interface of a decryption unit formed on a

monolithic semiconductor integrated circuit, the semiconductor integrated circuit comprising a common key store and a processing unit;

decrypting the encrypted broadcast common key utilizing a stored secret key in a secret key store in the semiconductor integrated circuit to generate a decrypted common key;

storing the decrypted common key in the common key store in the semiconductor integrated circuit;

decrypting the encrypted control signals with the common key to generate decrypted control signals;

providing the control signals to the processing unit; and

decrypting the encrypted broadcast signals using the processing unit in accordance with the control signals and providing decrypted broadcast signals to an output interface of the decryption device;

whereby the semiconductor integrated circuit is arranged such that the only route to placing a decrypted common key in the common key store is to ~~input~~ receive by broadcast the common key in encrypted form for decryption in accordance with the secret key and provide the decrypted common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to input them in encrypted form for decryption in accordance with the common key.

14. (Original) The method of claim 13, further comprising storing a secret key that is unique to the decryption unit in a secret key store in the decryption unit.

15. (Original) The method of claim 13, further comprising receiving multiple encrypted common keys, decrypting each of the encrypted common keys to generate multiple decrypted common keys, and storing the multiple decrypted common keys in a common key store in the decryption unit.

16. (Currently Amended) A method for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals that include picture and sound components, the method comprising:

encrypting control words and ~~transmitting~~ broadcasting the encrypted control words;

encrypting a common key and ~~transmitting~~ broadcasting the encrypted common key;

encrypting broadcast signals and ~~transmitting~~ broadcasting the encrypted broadcast signals to the plurality of subscribers;

providing a secret key to each authorized recipient that is stored in a secret key store on a monolithic semiconductor integrated circuit in a respective decryption unit;

receiving encrypted broadcast signals, encrypted broadcast control signals, and encrypted broadcast common key signals at an input interface of a decryption unit formed on the monolithic semiconductor integrated circuit, the semiconductor integrated circuit comprising a common key store and a processing unit;

decrypting the encrypted common key utilizing a stored secret key to generate a decrypted common key;

storing the decrypted common key in ~~the~~ a dedicated common key store on the monolithic semiconductor integrated circuit;

decrypting the encrypted control signals with the decrypted common key to generate decrypted control signals;

providing the control signals to the processing unit; and

decrypting the encrypted broadcast signals using the processing unit in accordance with the control signals and providing decrypted broadcast signals to an output interface of the decryption device;

whereby the semiconductor integrated circuit is arranged such that the only route to placing a common key in the common key store is to ~~input~~ receive by broadcast the common key in encrypted form for decryption in accordance with the secret key and provide the common key to the common key store over an internal bus, and the only route to providing the control

signals to the processing unit is to ~~input~~ receive by broadcast them in encrypted form for decryption in accordance with the common key.

17. (Original) The method of claim 16, further comprising storing a secret key that is unique to the decryption unit in a secret key store in the decryption unit.

18. (Original) The method of claim 16, further comprising receiving multiple encrypted common keys, decrypting each of the encrypted common keys to generate multiple decrypted common keys, and storing the multiple decrypted common keys in a common key store in the decryption unit.

19. (Currently Amended) A system for broadcasting signals to a plurality of subscribers in which only authorized recipients are able to decrypt the broadcast signals that include picture and sound components, the system comprising:

a transmitter configured to broadcast signals encrypted according to control words, to broadcast control words encrypted according to a common key that is common to two or more authorized recipients, and ~~a~~ to broadcast the common key encrypted according to a secret key that is unique to each authorized recipient; and

a plurality of receivers configured to receive the broadcast signals, each receiver comprising:

a common key store formed on a single monolithic semiconductor integrated circuit and configured to receive ~~a~~ the broadcasted common key;

a secret key store formed on a single monolithic semiconductor integrated circuit and configured to store a secret key;

a decryption unit formed on a single monolithic semiconductor integrated circuit and comprising a first decryption circuit configured to receive the broadcasted encrypted control signals and to decrypt the encrypted control signals in accordance with ~~a~~ the common key from the common key store, and a second decryption circuit configured to receive the broadcasted common key in encrypted form and to decrypt the encrypted common key in

accordance with a secret key from the secret key store and to store the common key in the common key store; and

a processing unit formed on a single monolithic semiconductor integrated circuit and configured to receive encrypted broadcast signals and decrypt the encrypted broadcast signals in accordance with the decrypted control signals received from the decryption unit and to provide decrypted broadcast signals to an output interface;

whereby the system is arranged such that the only route to placing a common key in the common key store is to ~~input~~ receive by broadcast the common key in encrypted form for decryption in accordance with the secret key and provide the decrypted common key to the common key store over an internal bus, and the only route to providing the control signals to the processing unit is to ~~input~~ receive them by broadcast in encrypted form for decryption in accordance with the common key.

20. (Original) The system of claim 19, wherein the common key store is configured to store multiple common keys.

21. (Previously Presented) The system of claim 19, wherein the decryption device is formed on the a single semiconductor integrated circuit having an input interface for receipt of encrypted broadcast signals, encrypted control signals, and encrypted common keys, and an output interface for output of decrypted broadcast signals.